

STAYSAFU **AUDIT**

JULY 13TH, 2022

SHINRAI INU

TABLE OF CONTENTS

- I. SUMMARY
- II. OVERVIEW
- III. FINDINGS
 - A. **BLOC-1** : Use of block.timestamp
 - B. **CENT-1** : Centralization of major privileges
 - C. **EXT-1** : External protocol dependance
- IV. GLOBAL SECURITY WARNINGS
- V. DISCLAIMER

AUDIT SUMMARY

This report was written for **Shinrai Inu (SHINRAI)** in order to find flaws and vulnerabilities in the **Shinrai Inu** project's source code, as well as any contract dependencies that weren't part of an officially recognized library.

A comprehensive examination has been performed, utilizing Static Analysis, Manual Review, and **Shinrai Inu** Deployment techniques. The auditing process pays special attention to the following considerations:

- ❖ Testing the smart contracts against both common and uncommon attack vectors
- ❖ Assessing the codebase to ensure compliance with current best practices and industry standards
- ❖ Ensuring contract logic meets the specifications and intentions of the client
- ❖ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders
- ❖ Through line-by-line manual review of the entire codebase by industry expert

AUDIT OVERVIEW

PROJECT SUMMARY

Project name	Shinrai Inu
Description	Shinrai Inu is a BNB Chain token that generates passive income to holders, receiving a percentage of auto reflections on every transaction with a primary use case developing an easy to use dapp, dashboard and nft character collection with Staking features
Platform	BNB Chain
Language	Solidity
Codebase	https://bscscan.com/address/0xd397fcbd4fb3f8cd3b3053d7b3e418dc47d357ea#code

FINDINGS SUMMARY

Vulnerability	Total
● Critical	0
● Major	0
● Medium	2
● Minor	1

- Informational

0

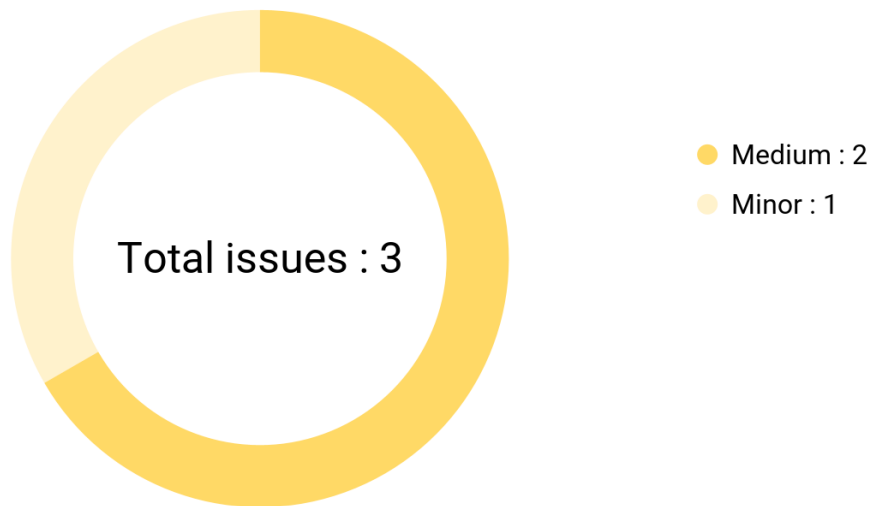
EXECUTIVE SUMMARY

Shinrai Inu is a **BEP20** token that powers the entire **Shinrai Inu** project, which includes NFTs, P2E game, and rewarding mechanisms. The token includes reflection mechanisms, splitted as it follows :

- Automatic burn **1%**
- Liquidity mechanism **2%**
- Marketing fee **4%**
- Reflections **1%**

There have been no major or critical issues related to the codebase and all findings listed in the process are informational or minor. The major security problems are the dependence on a decentralized exchange platform and the centralization of privileges.

AUDIT FINDINGS



Code	Title	Severity
CENT-1	Centralization of major privileges	● Medium
EXT-1	External protocol dependencies	● Medium
BLOC-1	Usage of block.timestamp	● Minor

BLOC-1 | Using block.timestamp

Description

The use of `block.timestamp` can be problematic. The timestamp can be partially manipulated by the miner (see <https://cryptomarketpool.com/block-timestamp-manipulation-attack/>). In this smart contract this is not critical as in the worst case an attacker could force the automatic liquidity mechanism to run faster or unpause the contract earlier.

Recommendation

We fully understand the smart contract's logic of the `Shinrai Inu token`. The use of `block.timestamp` is required to power the auto-liquify mechanism and we cannot replace it. Nevertheless, it is still useful to point out this kind of potential security problem.

CENT-1 | Centralization of major privileges

Description

The `onlyOwner` modifier of the smart contract gives major privileges over it (owner can change the marketing wallet address or exclude/include addresses from taxes)*. This can be a problem, in the case of a hack, an attacker who has taken possession of these privileged accounts could damage the project and the investors.

*This list is not exhaustive but presents the most sensitive points

Recommendation

We recommend at least to use a multi-sig wallet as the owner address, and at best to establish a community governance protocol to avoid such centralization. For more information, see <https://solidity-by-example.org/app/multi-sig-wallet/>

EXT-1 | Dependence to an external protocol

Description

The contract is serving as the underlying entity to interact with third party **PancakeSwap** protocols. The scope of the audit would treat this third party entity as black box and assume it is fully functional. However in the real world, third parties may be compromised and may have led to assets lost or stolen.

Recommendation

We encourage the team to constantly monitor the security level of the entire **PancakeSwap** project, as the security of the token is highly dependent on the security of the decentralized exchange platform.

Global security warnings

These are safety issues for the whole project. They are not necessarily critical problems but they are inherent in the structure of the project itself. Potential attack vectors for these security problems should be monitored.

CENT-1 | Global SPOF (Single Point Of Failure)

The project's smart contracts often have a problem of centralized privileges. The **owner** system in particular can be subject to attack. To address this security issue we recommend using a multi-sig wallet, establishing secure project administration protocols and strengthening the security of project administrators.

DISCLAIMER

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement.

This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement.

This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without StaySAFU's prior written consent. This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts StaySAFU to perform a security assessment.

This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance. This report should not be used in any way

to make decisions around investment or involvement with any particular project.

This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk.

StaySAFU's position is that each company and individual are responsible for their own due diligence and continuous security. StaySAFU's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or fun.